The Blackshades Global Takedown
Prepared Remarks of U.S. Attorney Preet Bharara
May 19, 2014

Good afternoon. My name is Preet Bharara, and I am the United States Attorney for the Southern District of New York.

Welcome to Cyber Monday. As you know, the cyber threat, in all of its forms, has been a top priority of law enforcement for several years – as you saw earlier this morning when the Attorney General announced a landmark case against Chinese government hackers for engaging in economic espionage.

And now, here in New York, we are announcing another global law enforcement operation that has exposed and crippled a frightening form of cybercrime, affecting hundreds of thousands of computer users around the world. It is a pernicious piece of software developed and sold by an organization known as Blackshades.

Blackshades' flagship product was a program known as the Remote Access Tool, or "RAT" for short. The RAT is inexpensive and simple to use, but its capabilities are sophisticated and its invasiveness breathtaking.

For just $40, the Blackshades RAT enabled anyone, anywhere in the world, to instantly become a dangerous cybercriminal – able to steal your property and invade your privacy.

Once installed on a victim's computer, the Blackshades RAT allowed users to remotely and secretly gain access to everything on a victim's computer, including private photographs and documents and passwords to online accounts. It could even record every keystroke entered on a victim's keyboard, to speedily steal credit card and other sensitive information.

Perhaps most disturbing, and taking the meaning of spyware to a new and more personal level, it even gave users the ability to activate a computer's camera to spy on a person in the victim's own home. All of this without the victim's knowledge.

The threat posed by Blackshades was far-reaching and global. Our investigation revealed that, over the past four years, the Blackshades RAT was purchased by users in over 100 countries, infecting more than half a million computers.

Our actions announced today take significant steps toward shutting down this threat and bringing those responsible to justice. We have charged three key members of the Blackshades organization, as well as two cybercriminals in the New York area who purchased the software and used it to victimize hundreds of innocent people.

Specifically, we announce charges against the two alleged creators of Blackshades RAT, Alex Yucel and Michael Hogue.

Yucel, a Swedish citizen, was arrested in Molodva in November 2013, and he is awaiting extradition to the United States. The indictment against Yucel had been under seal and was made public earlier today.

Hogue was arrested in Arizona in June 2012 and subsequently pled guilty in January 2013. Hogue has been cooperating with the Government in its investigation since his arrest.

We have also charged and arrested today (1) Brendan Johnston, a former Blackshades employee who helped market and sell the RAT, as well as provide technical assistance to its users, and (2) two New York-area purchasers of the RAT who allegedly used it to steal online account information and spy on victims through web cameras. They are Kyle Fedorek of Stony Point, New York, and Marlen Rappa of Middletown, New Jersey.

We have also seized the domain name for the Blackshades website, where the RAT software was sold, and obtained warrants to seize assets belonging to Blackshades' owner.

Before getting into additional details about the crimes alleged in the complaints and indictment unsealed today, let me introduce and thank our law enforcement team.

I am joined here today by our investigative partner in this and so many other extraordinary cybercrime cases – the FBI, represented here by Cyber Special Agent-in-Charge, Leo Taddeo.

I also want to recognize and thank Assistant Director-in-Charge of the New York Field Office, George Venizelos; Assistant Special Agent-in-Charge, Austin Berglas; Supervisory Special Agents Richard Jacobs and Andrew Cordiner; and Special Agents Patrick Hoffman, Mitchell Thompson, and Andy Dodd.

I also want to thank the career prosecutors in my office who have worked so tirelessly and creatively in this investigation. Specifically, I want to thank Jim Pastore and Sarah Lai, who lead this case, as well as the supervisors of the Complex Fraud and Cybercrime Unit, Richard Tarlowe and Nicky Friedlander, Serrin Turner, the Cybercrime Coordinator, and Paul Monteleoni of our Money Laundering and Asset Forfeiture Unit.

So, how did the Blackshades RAT work?

Getting this dangerous software was alarmingly simple. It was advertised on online computer hacker forums and it could easily be bought on Blackshades websites. Once purchased, the RAT user could install it on a victim's computer in a number of ways, including by tricking victims into clicking on links contained in emails or getting them to view a video or visit a website that would cause the malware to be installed.

Once a victim's computer was infected, a "spreader" feature could help disburse the infection to additional computers. For example, a user could set up the RAT to send an instant message to other potential victims. The message would invite the potential victim to click on a link that would lead to the recipient's computer getting infected.

To give potential victims a false sense of security, the instant message would appear as though it had come from someone with whom the victim regularly communicates.

What were some of the ways the Blackshades RAT wreaked havoc?

First, as I mentioned earlier, the Blackshades RAT enabled its users to intrude on the victim's privacy in the most sinister way: they could activate the victims' computer webcams to spy on and record them in the privacy of their own homes.

One of the defendants arrested today – Marlen Rappa – is alleged to have done just that.

Second, the RAT had a "keylogger" feature that recorded every keystroke on a victim's computer, as well as a "form grabber" feature which automatically captured all the information entered into electronic "forms," such as log-in screens or order-purchase screens, allowing its users to steal victims' passwords and other account information.

Using these tools, one of the defendants arrested today, Kyle Fedorek, allegedly used the RAT to steal online account information for more than 400 victims.

Third, the RAT had a tool known as the "file hijacker," which allowed RAT users to encrypt, or lock, a victim's files and then demand a "ransom" payment to unlock them.

As you can see the RAT even included a sample ransom note that could be sent to victims, saying "Your computer has basically been hijacked" and demanding payment in order for the computer to be "decrypted" and "restored."

Fourth, the RAT enabled its users to direct infected computers to carry out yet other cyberattacks. For example, infected computers could be gathered into a network and used to launch Distributed Denial of Service, or DDoS, attacks that could disable legitimate websites.

These threats posed by Blackshades knew no geographic boundaries. Nor did our investigative efforts. The scale and scope of international cooperation in this investigation has been remarkable and unprecedented.

In the United States alone, the FBI and our Office obtained court-authorized search warrants for more than 100 e-mail accounts and servers and seized more than 1,900 domain names used by RAT purchasers. And we worked closely with law enforcement agencies in over 19 countries, providing relevant information and leads to each, resulting in over 90 arrests and over 300 searches.

As I have said before, cybercrime is a global threat to both nations and individuals. And as the twin actions announced today make clear, it is without doubt one of the greatest threats facing our country. As today's case makes clear, we now live in a world where, for just $40, a cybercriminal halfway across the globe can – with just a click of a mouse – unleash a RAT that can spread a computer plague not only on someone's property, but also on their privacy and most personal spaces.

In such a world, the law enforcement community must be committed to confronting cybercrime with sustained dedication and creativity. And that is what we have done here. In the face of this gathering global threat, we will do what it takes and go where we need to protect the property and privacy of our citizens.